

CLAIMS

What is claimed is:

- 1 1. A method comprising:
2 receiving a network packet having a corresponding security association (SA);
3 determining for the packet a key value corresponding to the SA;
4 using the key value to determine a location of an entry in a lookup table, the entry
5 containing information corresponding to the SA;
6 retrieving from the entry an index to a location of the SA in memory; and
7 retrieving the SA from memory based on the index.
- 1 2. The method of claim 1 wherein receiving a network packet comprises a device
2 driver being passed an egress packet from an electronic system operating system.
- 1 3. The method of claim 1 wherein receiving a network packet comprises a device
2 driver being passed an ingress packet from a network interface device.
- 1 4. The method of claim 1 wherein the key value is a handle created for the SA
2 for an egress packet.
- 1 5. The method of claim 1 wherein the key value is a security parameter index
2 (SPI) extracted from the packet for an ingress packet.

1 6. The method of claim 1 wherein the lookup table entry comprises the key value
2 and the index.

1 7. The method of claim 6 wherein the lookup table entry further comprises a
2 counter to track collisions for the entry.

1 8. The method of claim 1 further comprising the location in memory of an SA
2 corresponding to egress traffic being in a first table, and the location in memory of an SA
3 corresponding to ingress traffic being in a second table.

1 9. The method of claim 1 further comprising an entry containing information for
2 an SA corresponding to egress traffic being in a first lookup table, and an entry containing
3 information for an SA corresponding to ingress traffic being in a second lookup table.

1 10. The method of claim 1 further comprising supporting a number of network
2 traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the
3 lowest binary number greater than five times the number of network traffic streams
4 supported.

1 11. The method of claim 1 wherein the key value is determined by using a bit-
2 wise AND hash function with a mask of value 2^N-1 , where N is an integer, wherein the hash
3 table contains 2^N entries.

1 12. An article comprising a machine-accessible medium to provide content to
2 cause one or more electronic systems to:
3 receive a network packet having a corresponding security association (SA);
4 determine for the packet a key value corresponding to the SA;
5 use the key value to determine a location of an entry in a lookup table, the entry
6 containing information corresponding to the SA;
7 retrieve from the entry an index to a location of the SA in memory; and
8 retrieve the SA from memory based on the index.

1 13. The article of claim 12 wherein to receive a network packet comprises a
2 device driver to be passed an egress packet from an electronic system operating system.

1 14. The article of claim 12 wherein to receive a network packet comprises a
2 device driver to be passed an ingress packet from a network interface device.

1 15. The article of claim 12 wherein the key value is a handle created for the SA
2 for an egress packet.

1 16. The article of claim 12 wherein the key value is a security parameter index
2 (SPI) extracted from the packet for an ingress packet.

1 17. The article of claim 12 wherein the lookup table entry comprises the key value
2 and the index.

1 18. The article of claim 17 wherein the lookup table entry further comprises a
2 counter to track collisions for the entry.

1 19. The article of claim 12 further comprising the location in memory of an SA
2 corresponding to egress traffic being in a first table, and the location in memory of an SA
3 corresponding to ingress traffic being in a second table.

1 20. The article of claim 12 further comprising an entry containing information for
2 an SA corresponding to egress traffic being in a first lookup table, and an entry containing
3 information for an SA corresponding to ingress traffic being in a second lookup table.

1 21. The article of claim 12 further comprising to support a number of network
2 traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the
3 lowest binary number greater than five times the number of network traffic streams
4 supported.

1 22. The article of claim 12 wherein the key value is to be determined by using a
2 bit-wise AND hash function with a mask of value 2^N-1 , where N is an integer, wherein the
3 hash table contains 2^N entries.

1 23. An electronic data signal embodied in a data communications medium shared
2 among a plurality of network devices comprising content to cause one or more electronic
3 systems to:

4 receive a network packet having a corresponding security association (SA);
5 determine for the packet a key value corresponding to the SA;
6 use the key value to determine a location of an entry in a lookup table, the entry
7 containing information corresponding to the SA;
8 retrieve from the entry an index to a location of the SA in memory; and
9 retrieve the SA from memory based on the index.

1 24. The electronic data signal of claim 23 wherein to receive a network packet
2 comprises a device driver to be passed an egress packet from an electronic system operating
3 system.

1 25. The electronic data signal of claim 23 wherein to receive a network packet
2 comprises a device driver to be passed an ingress packet from a network interface device.

1 26. The electronic data signal of claim 23 wherein the key value is a handle
2 created for the SA for an egress packet.

1 27. The electronic data signal of claim 23 wherein the key value is a security
2 parameter index (SPI) extracted from the packet for an ingress packet.

1 28. The electronic data signal of claim 23 wherein the lookup table entry
2 comprises the key value and the index.

1 29. The electronic data signal of claim 28 wherein the lookup table entry further
2 comprises a counter to track collisions for the entry.

1 30. The electronic data signal of claim 23 further comprising the location in
2 memory of an SA corresponding to egress traffic being in a first table, and the location in
3 memory of an SA corresponding to ingress traffic being in a second table.

1 31. The electronic data signal of claim 23 further comprising an entry containing
2 information for an SA corresponding to egress traffic being in a first lookup table, and an
3 entry containing information for an SA corresponding to ingress traffic being in a second
4 lookup table.

1 32. The electronic data signal of claim 23 further comprising to support a number
2 of network traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N
3 being the lowest binary number greater than five times the number of network traffic streams
4 supported.

1 33. The electronic data signal of claim 23 wherein the key value is to be
2 determined by using a bit-wise AND hash function with a mask of value 2^N-1 , where N is an
3 integer, wherein the hash table contains 2^N entries.

1 34. An electronic system comprising:
2 one or more processors;
3 a network interface coupled with the one or more processors to provide a
4 communications path between the electronic system and a network; and
5 a memory coupled with the one or more processors, the memory to have a program to
6 receive a network packet having a corresponding security association (SA), the program to
7 determine for the packet a key value corresponding to the SA, to use the key value to
8 determine a location of an entry in a lookup table, the entry containing information
9 corresponding to the SA, to retrieve from the entry an index to a location of the SA in
10 memory, and to retrieve the SA from memory based on the index.

1 35. The electronic system of claim 34 wherein the program to receive a network
2 packet comprises a device driver corresponding to the network interface, the device driver to
3 be passed an egress packet from an operating system.

1 36. The electronic system of claim 34 wherein the program to receive a network
2 packet comprises a device driver corresponding to the network interface, the device driver to
3 be passed an ingress packet from the network interface.

1 37. The electronic system of claim 34 wherein the key value is a handle created
2 for the SA for an egress packet.

1 38. The electronic system of claim 34 wherein the key value is a security
2 parameter index (SPI) extracted from the packet for an ingress packet.

1 39. The electronic system of claim 34 wherein the lookup table entry comprises
2 the key value and the index.

1 40. The electronic system of claim 39 wherein the lookup table entry further
2 comprises a counter to track collisions for the entry.

1 41. The electronic system of claim 34 further comprising the location in memory
2 of an SA corresponding to egress traffic being in a first table, and the location in memory of
3 an SA corresponding to ingress traffic being in a second table.

1 42. The electronic system of claim 34 further comprising an entry containing
2 information for an SA corresponding to egress traffic being in a first lookup table, and an
3 entry containing information for an SA corresponding to ingress traffic being in a second
4 lookup table.

1 43. The electronic system of claim 34 further comprising the program to support a
2 number of network traffic streams, wherein the lookup table has 2^N entries, where N is an
3 integer, 2^N being the lowest binary number greater than five times the number of network
4 traffic streams supported.

- 1 44. The electronic system of claim 34 wherein to hash the key value is to be
2 determined by using a bit-wise AND hash function with a mask of value 2^N-1 , where N is an
3 integer, wherein the hash table contains 2^N entries.